AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method comprising:

    initializing a pseudo-random number generator (PRNG);

    obtaining local seeding information from a host;

    securely obtaining additional seeding information from one or more remote

    entropy servers, wherein the securely obtaining of the seeding information

    from the one or more remote entropy servers is repeated for redundant

    entropy servers; and

    stirring the PRNG with the local seeding information and the additional seeding

    information.

2. (Previously Amended) The method of claim 1, wherein the initializing of the

    PRNG comprises initializing an internal state of the PRNG with a random value.

3. (Previously Amended) The method of claim 2, wherein the random value

    comprises a seed.

4. (Cancelled)

5. (Previously Amended) The method of claim 1, wherein the one or more remote

    entropy servers maintain random state pool to supply the host with the random

    value.

6. (Previously Amended) The method of claim 1, wherein the securely obtaining of

    the seeding information from the one or more remote entropy servers includes

    using a privacy protocol.

7. (Original) The method of claim 6, wherein the privacy protocol comprises secure

    sockets layer (SSL) protocol.

8. (Original) The method of claim 6, wherein the privacy protocol comprises transport layer security (TLS) protocol.

9. (Previously Amended) The method of claim 1, wherein the stirring of the PRNG comprises producing a cryptographically random stream of bits.

Claims 10-16 (Cancelled)

17. (Currently Amended) An entropy enhancing system comprising:

a local system ~~comprising~~ including a host and ~~, the local system further~~

~~comprising~~ a pseudo-random number generator (PRNG), the local system

to

initialize the PRNG~~, to obtain~~ by obtaining local seeding information from

the host,

securely obtain additional seeding information from one or more remote

entropy servers, and

~~stirring~~ stir the PRNG with the local seeding information and the

additional seeding information; and

the one or more remote systems ~~comprising~~ including the one or more entropy

servers to securely provide the additional seeding information to the local

system, wherein the securely providing of the additional seeding

information to the local system from the one or more entropy servers is

repeated for redundant entropy servers.

18. (Currently Amended) The entropy enhancing system of claim 17, wherein the

local system ~~to generate~~ generates the local seeding information at the host.

19.   (Currently Amended) The entropy enhancing system of claim 17, wherein the one or more remote systems ~~to generate~~generates the remote seeding information at the one or more entropy servers.

20.   (Previously Amended) The entropy enhancing system of claim 17, wherein the entropy servers comprise one or more of the following: hardware and software.

Claims 21-24 (Cancelled)

25.   (Currently Amended) A machine-readable medium having stored thereon data ~~comprising~~representing sets of instructions which, when executed by a machine, cause the machine to:

initialize a pseudo-random number generator (PRNG);

obtain local seeding information from a host;

securely obtain additional seeding information from one or more remote entropy servers, wherein the securely obtaining of the seeding information from the one or more remote entropy servers is repeated for redundant entropy servers; and

stir the PRNG with the local seeding information and the additional seeding information.

26.   (Previously Amended) The machine-readable medium of claim 25, wherein the initializing of the PRNG comprises initializing an internal state of the PRNG with a random value.

27.   (Previously Amended) The machine-readable medium of claim 26, wherein the random value comprises a seed.

28.   (Cancelled)

29.   (Previously Amended) The machine-readable medium of claim 25, wherein the one or more remote entropy servers maintain random state pool to supply the host with the random value.

30.   (Previously Amended) The machine-readable medium of claim 25, wherein the stirring of the PRNG comprises producing a cryptographically random stream of bits.